U.S. Department of Justice

United States Attorney
Eastern District of New York

AB:SSS/GMM
F.#2016R02185

271 Cadman Plaza East
Brooklyn, New York 11201

August 23, 2019

By Hand and ECF

Honorable Kiyo A. Matsumoto
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, NY 11201

Re: United States v. Ingrid Innes
Criminal Docket No. 18-134 (S-2)(KAM)

Dear Judge Matsumoto:

The government respectfully submits this motion to request that the Court find that a document created by Ingrid Innes (the "Document"), the above-referenced defendant, is not protected by the attorney-client privilege. While Innes has not yet been arrested, the government requests a ruling prior to the trial of her co-defendant, Donville Inniss, which is scheduled to begin on October 28, 2019. The government will provide a copy of the Document, which is labeled as Exhibit A, as well as the other exhibits described below, under seal for in-camera review by the Court.

I. Background

The defendant is charged in a Second Superseding Indictment (the "Indictment") with one count of conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h), and two substantive counts of money laundering, in violation of 18 U.S.C. § 1956(a)(2)(A).

The government expects the evidence to show that the defendant, who was the Chief Executive Officer ("CEO") of the Insurance Corporation of Barbados Ltd. ("ICBL" or the "Company") during the relevant time period, engaged in a bribery and money laundering scheme through which she paid bribes to co-defendant Donville Inniss, who was a member of the Parliament of Barbados and the Minister of Industry, International Business, Commerce, and Small Business Development of Barbados (the "Minister of Industry") in 2015 and 2016. Innes, together with co-defendant Alex Tasker, then-Senior Vice President of ICBL, then laundered the bribe payments to and through the United States and elsewhere. In exchange for these bribe payments, Inniss used his position as Minister of Industry to cause the Barbados Investment and Development Corporation, a Barbadian government agency, to renew insurance contracts with ICBL.

To covertly receive the bribe payments from ICBL, Inniss arranged to launder the bribes through a bank account in New York in the name of a dental company (the "New York

Dental Company"), which had no actual business with ICBL. The New York Dental Company then transferred the bribe payments to Inniss' personal bank accounts in the United States. Overall, Inniss received approximately $36,000 in bribe payments from ICBL through bank accounts in the United States.

On or about October 5, 2016, John Wight, the President and CEO of BF&M Limited, ICBL's parent company, suspended the defendant after he received information indicating that she had participated in the scheme. See Ex. B, Email from Wight to Wight, at 1. At that time, Mr. Wight informed the defendant that the ICBL Board of Directors was conducting an "independent investigation" into whether she had bribed a Barbadian official. See id.

According to metadata produced by ICBL, the defendant created the Document on or about October 9, 2016. See Ex. C, Document Metadata, at 1. By this time, the defendant had been suspended and was neither present in the ICBL office, nor working from home. See Ex. D, Emails Between Wight and Innes, at 4. The metadata shows that the defendant saved the Document as a Microsoft Word file in a folder called "Documents." See Ex C at 1. According to ICBL, the defendant created and stored the Document, which was not password protected, using a tablet computer that ICBL owned and issued to her in connection with her employment. The Document, which describes certain facts relevant to the case, nowhere indicates that it is an attorney-client communication. See Ex. A. Further, the defendant was not an attorney.

On or about October 22, 2016, Mr. Wight emailed the defendant that she was not permitted to return to the ICBL office while she was suspended and that ICBL's lawyers may want to interview her. See Ex. D at 6-7. On or about October 23, 2016, Mr. Wight emailed the defendant that "during the suspended period, the company issued laptop and phone [must] be returned to the company." Id. at 5. On or about October 24, 2016, the defendant responded by email to Mr. Wight, "I also have personal emails on my desktop at the office which I have not touched and would appreciate some consideration with this." Id. at 4. The next day, Mr. Wight informed the defendant by email that she was required to allow the accounting firm "KPMG, who are advising the Board of Directors of ICBL, to secure and image your Company issued laptop and mobile device." Id. at 2-3. He also explained that KPMG "will require any passwords to gain access to the data." Id. at 3. On or about October 26, 2016, the defendant emailed Mr. Wight that she "[j]ust realized that [she had] an IPad also" and that she would "deliver [it] to kpmg." See Ex. E, Emails Between Wight and Innes, at 1. According to ICBL, the defendant ultimately provided KPMG with the tablet computer that ICBL had issued to her and KPMG then found the Document while searching the tablet for information relevant to ICBL's internal investigation. ICBL has informed the government that the defendant did not delete the Document from the tablet computer before turning it over to KPMG.

ICBL's Code of Ethics and Business Conduct in place in October 2016 (the "Code") provides that the use of "Company resources, such as time, material, equipment and information, are provided for Company business use," and further that "Company equipment such as computers, copiers and fax machines must not be used in the conduct of an outside business or in support of any religious, political or other outside daily activity, except for Company-requested support to non-profit organizations." Ex. F, Code of Conduct ¶¶ 1.11.1, 1.11.3. The Code further states, "[i]n order to protect the interests of our network and our fellow employees, the Company reserves the right to monitor or review all data and information

contained on an employee's Company-issued computer or electronic device, and the use of the Internet or intranet." Id. ¶ 1.11.4. It also bans any objectionable or harassing use of such equipment. Id. The Code is prefaced by a letter from the defendant to the other employees of ICBL in which she writes, "Please read this Code carefully . . . . [and] [r]efer to it often . . . ." Id. at 1. The Code's prefatory letter from the defendant also states that employees of ICBL must sign an acknowledgement enclosed in the Code. Id. The Code also provides that "[i]t is the added responsibility of Management to consistently demonstrate, through their actions, the importance of this Code." Id. ¶ 1.3.1.

A letter from ICBL's outside counsel to the government states that ICBL "monitors Company-issued computer and electronic devices, including tablets, when a breach of Company policy is suspected, when requested by senior management, and in other circumstances as appropriate." Ex. G, June 9, 2017 Letter, at 1. The letter also states that "ICBL's IT administrators can monitor and access data on Company-issued computer and electronic devices, including tablets, remotely when such devices are connected to the corporate network . . . . [and that] ICBL could have remotely monitored and accessed [the Document] that the metadata shows was stored in the 'My Documents' folder on the tablet, for example, via an established VPN connection." Id. at 1-2. In addition, the letter states that ICBL understood that "Ms. Innes had previously made requests of ICBL's IT administrators to monitor other employees' Company-issued technology in other contexts." Id. at 2.

ICBL's outside counsel voluntarily produced the Document to the government on or about December 9, 2016. Subsequently, according to ICBL, during an interview with KPMG in late December 2016, Innes claimed for the first time that the Document was created for her attorney and was privileged. Innes then retained a U.S. lawyer who engaged in discussions with the government about the government's investigation. On or about March 22, 2017, the government informed Innes' counsel that ICBL had produced the Document to the government prior to her claiming that it was privileged and explained why the government did not believe that the Document was privileged. The government recommended to Innes' attorney that he make a motion to the Miscellaneous District Judge in the Eastern District of New York if the defendant continued to assert privilege over the document. Instead of filing a motion, on May 10, 2017, the defendant sent a letter to the government asserting privilege over the Document and asking the government to destroy all copies of the Document. On December 14, 2017, the government sent a letter in response to the defendant explaining the government's position that the Document is not protected by the attorney-client privilege, and again suggesting that the defendant make a motion in the Eastern District of New York if she continued to assert privilege over the Document. To date, the defendant has not filed any motion in this Court claiming privilege over the Document, even after the charges against her became public in January 2019.

While the government continues to assert that the Document is not privileged, out of an abundance of caution, the government has not used the Document in connection with its investigation or prosecution of the three defendants named in the Indictment. The government also has not produced the Document to defendant Donville Inniss in discovery.

II. Applicable Law and Analysis

The attorney-client privilege protects "(1) a communication between client and counsel that (2) was intended to be and was in fact kept confidential, and (3) was made for the purpose of obtaining or providing legal advice." In re County of Erie, 473 F.3d 413, 419 (2d Cir. 2007) (citation omitted). The Document does not meet this test for two reasons.

First, the Document was not confidential because the defendant created it using a Company-issued tablet computer and maintained a copy of it on that computer. The Second Circuit has not "specifically addressed the extent to which information stored on an employer's computer system can be a confidential communication for purposes of the attorney-client privilege." Orbit One Commc'ns, Inc. v. Numerex Corp., 255 F.R.D. 98, 107-108 (S.D.N.Y. 2008). Courts have thus "sought to determine whether the employee, as a practical matter, had a reasonable expectation that the attorney-client communications would remain confidential despite being stored on a company's computer system." United States v. Hatfield, No. 06-CR-0550 (JS), 2009 WL 3806300, at *8 (E.D.N.Y. Nov. 13, 2009).

> In assessing an employee's reasonable expectation of privacy in a work computer or e-mail account, courts have increasingly turned to a set of four factors: " '(1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?' "

United States v. Finazzo, No. 10-CR-457 (RRM), 2013 WL 619572, at *7 (E.D.N.Y. Feb. 19, 2013) (quoting In re the Reserve Fund Sec. & Deriv. Litig., 275 F.R.D. 154, 160 (S.D.N.Y. 2011) (quoting In re Asia Global Crossing, LTD., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005))), aff'd by United States v. Finazzo, 682 F. App'x 6, 15-16 (2d Cir. 2017) (affirming district court ruling that emails between defendant and his attorney that defendant sent and received using work email system were not privileged where employer policies stated that employees had no expectation of privacy when using company systems, the company reserved the right to monitor use of company systems, and the defendant acknowledged he had read the employee handbook that contained the policies).

Here, each of these factors supports a finding that the Document was not confidential.

- First, ICBL had a policy banning personal and objectionable use of its computers. The Code stated that "Company resources, such as . . . equipment . . . are provided for Company business use" and that Company-issued computers "must not be used . . . in support of any . . . outside daily activity" – which would include communications with a personal attorney – or for any objectionable or harassing uses. Ex. F, Code of Conduct ¶¶ 1.11.1, 1.11.3, 1.11.4.

- Second, ICBL monitored the use of Company-issued computers. The Code stated that "he Company reserves the right to monitor or review all data and information contained

on an employee's Company-issued computer or electronic device, and the use of the Internet or intranet." Id. ¶ 1.11.4. ICBL has also informed the government that it did, in fact, monitor Company-issued computers and the use of the Internet. See Ex. G at 1. In fact, when she was the CEO of ICBL, the defendant herself had apparently made requests of ICBL's Information Technology administrators to monitor other employees' Company-issued technology in other prior contexts. Id. at 2.

- Third, although ICBL does not "as a general matter grant[] third parties a regular right of access to Company-issued technologies," id. at 2, on or about October 5, 2019, four days before she created the Document, the defendant was suspended and informed that the ICBL Board of Directors was conducting an "independent investigation" of her actions. Ex. B at 1. At the time when the defendant created the Document, it was thus reasonably foreseeable that ICBL could have chosen to grant a third party such as KPMG access to the tablet that contained the Document in connection with its "independent" investigation, which ICBL, in fact, ultimately did in this case.

- Finally, ICBL informed the defendant of these policies. Indeed, the defendant authored a prefatory letter requiring all ICBL employees to read and adhere to the Code. The defendant was also well aware that ICBL monitored employee-issued technology because she apparently requested that ICBL monitor the technology of other employees. Id. at 2.

In light of these factors, the defendant did not have a reasonable expectation that the Document was confidential. See, e.g., United States v. Nordlicht, No. 16-CR-640 (BMC), 2018 WL 705548, at *4-5 (E.D.N.Y. Feb. 2, 2018) (finding, in the Fourth Amendment context, that defendants did not have a reasonable expectation of privacy in use of company-issued electronic devices where, among other things, the company instructed employees to "minimize" use of such devices for personal use, reserved the right to monitor the devices, and informed the defendants of these policies); In re Reserve Fund Sec., 275 F.R.D. at 163 ("Where an employer reserves the right to access or inspect an employee's email or work computer, courts often find that the employee has no reasonable expectation of privacy.").

Second, even if the Document were confidential – which it was not – the defendant waived the attorney-client privilege with respect to the Document. "It is well-established that voluntary disclosure of confidential material to a third party waives any applicable attorney-client privilege." Schanfield v. Sojitz Corp. of Am., 258 F.R.D. 211, 214 (S.D.N.Y. 2009) (citing United States v. Jacobs, 117 F.3d 82, 91 (2d Cir. 1997)). Here, the defendant voluntarily provided the tablet computer to KPMG at a time when she knew that KPMG was assisting ICBL's Board of Directors with an independent, internal investigation into the same facts described in the Document. The defendant neither deleted the Document nor took any other steps to inform KPMG or ICBL that there were communications with her attorney saved on the tablet computer.

The situation here is therefore distinguishable from the one in Curto v. Med. World Commc'ns, Inc., No. 03-CV-6327 (DRH) (MLO), 2006 WL 1318387 (E.D.N.Y. May 15, 2006). In Curto, the court found that the employee had a reasonable expectation of privacy in a document she created on a laptop she was using in a home office, where the company did not

have access to the documents. Id. at *5-6.[1] Unlike here, however, the employee in Curto deleted her communications with counsel from her company-issued laptop before returning it to her employer, and the emails were only recovered from the deleted files during a forensic audit. See In re Reserve Fund Sec., 275 F.R.D. at 162 (distinguishing Curto by noting, among other things, that "the court ruled that plaintiff—in deleting her personal files from the laptops—had taken reasonable steps to ensure the confidentiality of her attorney-client communications"). In addition, Curto – an employee of her company – was legitimately using her work computer when she created the documents at issue in that case because she was working from a home office. By contrast, the defendant here, who was the CEO of her company, created the Document four days after being suspended and informed that she was under investigation for the very issues described in the Document. Accordingly, even if the Document were confidential, the defendant would have waived any attorney-client privilege that she may have had over the Document when she voluntarily provided the tablet computer containing the Document to KPMG approximately two weeks after she had created it, and failed to assert any privilege or take any other precautions to protect any privacy interest in the Document. See, e.g., Aventa Learning, Inc. v. K12, Inc., 830 F. Supp. 2d 1083, 1106 (W.D. Wash. 2011) (finding that employee waived the attorney-client privilege when he relinquished his company-issued laptop computer to his employer "without asserting privilege or taking any precautions to protect the privacy of the materials he had saved on the laptop").

For the above reasons, the Document is not protected by the attorney-client privilege.

[1] Here, according to ICBL, the Company's Information Technology department would have had the ability to monitor the Document if the defendant had logged into ICBL's system remotely using a VPN network. See Ex. G at 1.

III. Conclusion

For the reasons set forth above, the government's request that this Court find that the Document is not protected by the attorney-client privilege should be granted, and the government should be permitted to use the Document in its prosecution of the defendant and produce it to the defendant Donville Inniss in discovery.

Respectfully submitted,

RICHARD P. DONOGHUE
United States Attorney

By: /s/
Sylvia Shweder
Assistant U.S. Attorney
(718) 254-6092

ROBERT A. ZINK
Chief, Fraud Section
Criminal Division
U.S. Department of Justice

By: /s/
Gerald M. Moody, Jr.
Trial Attorney
U.S. Department of Justice
(202) 616-4988

Enclosures filed under seal

cc: Ronald G. DeWaard, Esq., counsel to Ingrid Innes (by email, with enclosures)